#4

EL896636040US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Graeme John PROUDLER, et al.
Serial No.: Not yet assigned) Group: Not yet assigned
Filed: Concurrently herewith) Examiner: Not yet assigned
) Our Ref: B-4515 619561-7
For: "INFORMATION SYSTEM") Date: February 22, 2002

CLAIM TO PRIORITY UNDER 35 U.S.C. 119

Commissioner of Patents and Trademarks
Box New Patent Application
Washington, D.C. 20231

Sir:

[X] Applicants hereby make a right of priority claim under 35 U.S.C. 119 for the benefit of the filing date(s) of the following corresponding foreign application(s):

COUNTRY	FILING DATE	SERIAL NUMBER
Great Britain	23 February 2001	0104584.8

[ ] A certified copy of each of the above-noted patent applications was filed with the Parent Application No.________________________.

[X] To support applicant's claim, a certified copy of the above-identified foreign patent application is enclosed herewith.

[ ] The priority document will be forwarded to the Patent Office when required or prior to issuance.

Respectfully submitted,

Richard P. Berg
Attorney for Applicant
Reg. No. 28,145

LADAS & PARRY
5670 Wilshire Boulevard
Suite 2100
Los Angeles, CA 90036
Telephone: (323) 934-2300
Telefax: (323) 934-0202

PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
The Patent Office

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 2 May 2001

Patents Form 1/77

Patents Act 1977
(Rule 16)

The Patent Office

1/77

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

1. Your reference — 30007644 GB

2. Patent application number *(The Patent Office will fill in this part)* — 0104584.8

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Hewlett-Packard Company
3000 Hanover Street
Palo Alto
CA 94304, USA

Patents ADP number *(if you know it)* — 00496588001

If the applicant is a corporate body, give the country/state of its incorporation — Delaware, USA

4. Title of the invention — Information System

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Richard A. Lawrence
Hewlett-Packard Ltd, IP Section
Filton Road
Stoke Gifford
Bristol BS34 8QZ

Patents ADP number *(if you know it)* — 07448038001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

Yes

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	18
Claim(s)	2
Abstract	1
Drawing(s)	6 +6

8

10. If you are also filing any of the following, state how many against each item.

Priority documents	-
Translations of priority documents	-
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	1 ✓
Request for preliminary examination and search *(Patents Form 9/77)*	1 ✓
Request for substantive examination *(Patents Form 10/77)*	-
Any other documents *(please specify)*	Fee Sheet ✓

11. I/We request the grant of a patent on the basis of this application.

Signature Richard A. Lawrence

Date 22/02/01

12. Name and daytime telephone number of person to contact in the United Kingdom

Meg Joyce Tel: 0117-312-9068

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

INFORMATION SYSTEM

Field of the Invention

This invention relates to an information system and, in particular, to a system for providing information relating to a predetermined geographical area.

Background to the Invention

Conventional prior art mass market computing platforms include personal computers, server computers, information appliances, communication devices, display devices, hard copy devices, and the like.

There is substantial potential, at least in theory, for widespread interaction between such computing platforms. However, because of the potential for fraud and manipulation of electronic data, such interaction and, in particular, fully automated transactions between such computing platforms are often avoided. The fundamental issue is one of trust between interacting computer platforms.

There have been several prior art schemes which are aimed at increasing the security and trustworthiness of computing platforms. Predominantly, these rely upon adding in security features at the application level, as opposed to building them into the fundamental hardware components of the computing platform, and although such prior art schemes go some way to improving the security of computer platforms, the levels of security and trust gained thereby may be considered insufficient for some applications in which greater confidence in the trustworthiness of the underlying technology may be required.

In the applicant's co-pending International Patent Application Publication No. PCT/GB00/00528 entitled 'Trusted Computing Platform', filed on 15 February 2000, and International Patent Application No. PCT/GB00/00751 'Computing Apparatus and Methods of Operating Computing Apparatus' filed on 3 March 2000, the entire contents of which are incorporated herein by reference, there is disclosed a concept of a 'trusted computing platform' comprising a computing platform which has a 'trusted component' in the form of a built-in hardware and software component. Two computing entities each provisioned with such a trusted component may interact with each other with a high degree of 'trust'. That is to say, where the first and second computing entities interact with each other, the security of the transaction enhanced compared to the case where no trusted component is present, because:

- A user of a computing entity has higher confidence in the integrity and security of his/her own computer entity and in the integrity and security of the computer entity belonging to the other computing entity.
- Each entity is confident that the other entity is in fact the entity which it purports to be.
- Where one or both of the entities represent a party to a transaction, e.g. a data transfer transaction, because of the built-in trusted component, third party entities interacting with the entity have a high degree of confidence that the entity does in fact represent such a party.

The trusted component increases the inherent security of the entity itself, through verification and monitoring processes implemented by the trusted component.

The computer entity is more likely to behave in the way it is expected to behave.

However, if a first computer platform user enters a geographical area, for example, a building, in which the computer platforms are unfamiliar to him/her, the security attributes of such computer platforms will also be unknown. Thus, the user will be unaware of the computer platforms available for use, and also the degree of confidence with which he/she may interact therewith.

Existing methods of providing or publishing security information include a "Public Key Infrastructure" and key distribution systems.

In a Public Key Infrastructure, a certificate states certain attributes of a target and is signed by some previously trusted entity. A visitor to, for example, a building, obtains a certificate and is able to verify the authenticity of the certificate because of prior knowledge of the trusted entity. The visitor trusts the trusted entity, and therefore trusts the attributes (including security attributes) stated in the certificate.

In known key distribution schemes, the visitor receives keys of a target from a key distribution service. The key distribution service is expected to trust the visitor, and vice versa. Keys may be expected to be trusted by the visitor because they are signed by the key distribution service, and the visitor is able to verify such signatures. Keys may be rendered confidential because of intimate contact with a node of the key distribution service. Alternatively, keys may be rendered confidential because they are encrypted by the key distribution service, and the visitor is able to decrypt such data.

Many predetermined areas have a central information point from which general information may be obtained by a visitor who is unfamiliar with that area. However, such information is usually only displayed on a screen for perusal by the visitor. There is usually no way of saving such information electronically in a user's computer platform, for example, for reference or use later, and even if there were, it is unlikely that the user would trust the integrity and security of the information point sufficiently to allow it to interact with his/her computer platform.

Summary of the Invention

In accordance with a first aspect of the invention, there is provided an information system comprising an information access point including means for retrieving information relating to computing platforms located within a predetermined area, together with security attributes thereof, and means for providing said information to a user upon request.

Thus, a visitor to a building, for example, who is unfamiliar with the computing platforms available for use therein can obtain such information from a central information access point. In a preferred embodiment, the system provides only details and/or a list of public keys of genuine trusted computing platforms within the area, i.e. those including a 'trusted component'. In this case, the information system preferably also comprises a trusted computing platform.

Beneficially, the information system comprises means for communicating or interacting with a user's portable computing apparatus. Such apparatus may be in the form of a smart card, such that the information system includes a smart card reader, or, for example, a laptop computer or the like. In any event, it is preferable for communications between the information system and the user's portable computer apparatus to be unambiguous, such that the system preferably comprises a contact reader or directional wireless communication such as IR, for example.

If the information system is for use within an area owned by a private organisation, the system preferably includes means for verifying the identity of the user. However, if the system is for use in a publicly-owned area, such as a library or government building, then the system may preferably be arranged to provide the requested information indiscriminately upon request.

The system may include means to enable the user to perform operations, either locally or remotely, upon the information provided thereby.

Thus, in summary, the first aspect of the present invention provides a trusted service which publishes information describing security attributes of computing platforms in a defined physical area. Distribution of the information preferably requires intimate contact with a node of the information system. The information system may be indiscriminate and provide information on demand to any user, it may require identification of a user before distributing the requested information. Of course, various levels of information may be available to different levels of authority.

In use, the information system is preferably presented to users accompanied by an explicit or implicit declaration by the provider of the service about the trustworthiness of the system and its information. Such a declaration may be implicit due to the physical location of the system within the predefined area and/or it may be explicit by virtue of a statement located on or near the system. The declaration may be the primary or only basis of trust in the system and its information and, as such, the user is expected to base his/her trust of the system upon the basis of such a declaration. The declaration is preferably capable of interpretation by a user without preprocessing by an information processing system.

The system may provide an additional restricted set of services to the user, which may optionally permit the user to perform tests (either locally or remotely) on the information, thereby to increase confidence in the information about the computing platforms in the predefined area. The system is preferably arranged to erase all memory of a user's use of the system, to preserve the user's privacy. Such memory may be erased after a predetermined period of time, or upon the user's exit from the predefined area or on command. The system may also be arranged to delete upon command any information in the user's personal computing apparatus that was previously provided to the user's personal computing apparatus.

In a most preferred embodiment of the first aspect of the invention, the set of described computing platforms provided by the information system is restricted to 'trusted computing platforms'. Thus, the information system may comprise a smartcard reader that contains a list of public keys that identify trusted platforms within the vicinity. The list would preferably be signed by the attesting entity. When a visitor to an area wishes to use a trusted computing platform within that area, the visitor can use their personal smartcard to obtain details of genuine trusted computing platforms in the area and, optionally, verify such details before using the platforms. The visitor's smartcard thereafter knows which platforms in the vicinity are genuine trusted platforms.

In accordance with a second aspect of the present invention, there is provided an information system comprising a computing platform having a trusted component, means for communicating with a user's portable computing apparatus, means for retrieving information relating to a predetermined area and communicating said information to said user's portable computing apparatus upon request.

Thus, the second aspect of the present invention provides a general information system which enables selected trustworthy information about an unfamiliar geographical area to be retrieved and distributed to a user's personal computing apparatus. Such information may relate to computing platforms within the area, as in the first aspect of the present invention, and the system may be arranged to provide a list of public keys of trusted computing platforms and/or a list of the public keys or the certificates of the public keys for other equipment. Thus, the system provides a key distribution service which may be implemented using a standard key distribution mechanism, for example, one of the mechanisms in ISO/IEC 11770. In addition, or alternatively, it may comprise information such as maps, contact information, shopping information, etc. depending upon the predefined area in which the system is located. Some or all of the provided information may also be displayed on a screen or monitor.

The user's personal computing apparatus may comprise a smartcard, in which case the system comprises a smartcard reader. However, the user's personal computing apparatus may alternatively comprise a PDA, mobile phone, USB token (i.e. a reader-less smartcard), and the like. The integrity of the information system computing platform can preferably be verified via the user's personal computing apparatus. In one embodiment of the invention, the system is preferably arranged to verify the identity of the user before providing the requested information.

Brief Description of the Drawings

An embodiment of the present invention will now be described by way of example only and with reference to the accompanying drawings, in which:

Figure 1 illustrates schematically a trusted computing platform as previously described in PCT/GB00/00528.

Figure 2 illustrates schematically connectivity of selected components of the computing platform of Figure 1;

Figure 3 illustrates schematically a hardware architecture of components of the computing platform of Figure 1;

Figure 4 illustrates schematically and architecture of a trusted component comprising the computing platform of Figure 1;

Figure 5 illustrates schematically a hardware architecture of components of an exemplary embodiment of an information system according to the present invention; and

Figure 6 illustrates schematically an exemplary embodiment of an information system according to the present invention.

Detailed Description of the Invention

In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art, that the invention may be practiced without limitation to these specific details. In other instances, well known methods and structures have not been described in detail so as to avoid unnecessarily obscuring the present invention.

Referring to Figure 1 of the drawings, there is illustrated schematically one example of a trusted computing platform as previously described in PCT/GB00/00528. Referring to Figure

2, there is illustrated schematically the physical connectivity of some of the components of the trusted computer platform of Figure 1. Referring to Figure 3, there is illustrated schematically an architecture of the trusted computing platform of Figures 1 and 2, showing physical connectivity of components of the platform. Referring to Figure 4, there is illustrated schematically an architecture of a trusted component included in the computer platform of Figure 1.

In the example shown in Figures 1 to 4, the trusted computing platform is shown in the form of a personal computer suitable for domestic or business use. However, it will be understood by those skilled in the art that this is just one specific example of a trusted computing platform, and other example may take the form of a palmtop computer, a laptop computer, a server-type computer, a mobile phone-type computer, information appliances, communication devices, display devices and hard copy devices generally, and the like, and the invention is limited only by the scope of the appended claims.

In the example illustrated by Figure 1, the computing platform comprises a display monitor 100, a keyboard data entry means 101, a casing 102 comprising a motherboard on which is mounted a data processor, one or more data storage means, a dynamic random access memory, various input and output ports (not illustrated in Figure 1), a smart card reader 103 for accepting a user's smart card, a confirmation key 104, which a user can activate when confirming a transaction via the trusted computing platform, and a pointing device, e.g. a mouse or trackball device 105 (the function of such a "trusted key" can also be implemented in software). The trusted computing platform also has a trusted component as described in the applicant's previous disclosure and as further described herein.

some of the components included in the trusted computing platform, including keyboard 101 which incorporates confirmation key 104 and a smart card reader 103, a main motherboard 200 on which is mounted first data processor 201 and trusted component 202, and example of a hard disk drive 203, and monitor 100. Additional components which may be included in the computing platform, such as an internal frame to the casing 102 housing one or more local area network (LAN) ports, one or more modem ports, one or more power supplies, cooling fans, and the like, are not shown in Figure 2.

Referring to Figure 3 of the drawings, main motherboard 200 is manufactured comprising a processor 201, and a preferably permanently fixed trusted component 202, a memory device 300 local to the processor, a BIOS memory area 301, smart card interface 305, a plurality of control lines 302, a plurality of address lines 303, a confirmation key interface 306, and a databus 304 connecting the processor 201, trusted component 202, memory area 300, BIOS memory area 301 and smart card interface 305. A hardware random number generator 309 is also able to communicate with the processor 201 using the bus 304.

External to the motherboard and connected thereto by the databus 304, are provided one or more hard disk drive memory devices 203, keyboard data entry device 101, pointing device 105, monitor 100, smart card reader 103, and one or more peripheral devices 307, 308, for example, a modem , printer, scanner, or other known peripheral device.

In the illustrated example, smart card reader 103 is wired directly to smart card interface 305 on the motherboard and does not connect directly to the databus 304. In an alternative example, however, the smartcard reader 103 may be connected directly to databus 304. To provide enhanced security, confirmation key switch 104 is hard wired directly to confirmation key interface 306 on motherboard 200, which provides a direct signal input to trusted component 202 when confirmation key 104 is activated by a user such that a user activation the confirmation key sends a signal directly to the trusted component, by-passing the first data processor and first memory means of the computer platform.

Trusted component 202 is positioned logically and physically between monitor 100. and processor 201 of the computing platform, so that trusted component 202 has direct control over the views displayed on monitor 100 which cannot be interfered with by processor 201.

Confirmation key 104 and confirmation key driver 306 provide a protected communication path (PCP) between a user and the trusted component, which cannot be interfered with by processor 201, which by-passes databus 304 and which is physically and logically unconnected to memory area 300 or hard disk drive memory device(s) 203.

The trusted component lends its identity and trusted processes to the computer platform and the trusted component has those properties by virtue of its tamper-resistance, resistance to forgery, and resistance to counterfeiting. Only selected entities with appropriate authorisation mechanisms are able to influence the processes running inside the trusted component. Neither an ordinary user of the trusted computer entity, nor any ordinary user or any ordinary entity connected via a network to the computer entity may access or interfere with the processes running inside the trusted component. The trusted component has the property of being "inviolate".

In the illustrated example, the trusted component operates to monitor data, including user data files and applications, on the computer platform by creating a set of data files which the trusted component dynamically monitors for any changes in the data, including absence of the data, which may occur as a result of the computer platform being compromised by a virus attack, or other interference. The trusted component is allocated or seizes a plurality of memory location addresses and/or file directories in the first memory area of the computer platform, which become a user space reserved for use by the trusted component.

The reserved memory area comprises a selected proportion of the total memory area of the computer platform. Within the reserved memory area, the trusted component also creates a plurality of data files, which can either be copies from real user data files on the computer platform, or which can be created by the trusted component. The primary purpose of these files is to act as a set of files to which the trusted component has access, and to which ordinary user accounts of the computer platform, under normal operation, do not have access. Because the files in the reserved memory area are reserved for use by the trusted component and under normal operation, are not accessed by applications on the computer platform, the trusted component can use files stored in the reserve memory area as a "control" set of files by which to monitor unauthorised changes to the data, for example as caused by a virus.

Because the files stored in the reserved memory area are either duplicates of user files, duplicates of applications or files created specifically by the trusted component, they are of little or no value to the computer platform for performing its normal operating functions. If the files in the reserve memory area become corrupted for any reason, they may be sacrificed and are easily replaceable. However, since access to the reserve memory area is restricted to the trusted component, any corruption of the files in the reserve memory area is deemed to be indicative of changes to files occurring through undesirable mechanisms, e.g. by a virus program. The files in the reserve memory area are periodically monitored by the trusted component to check for such corruption. If corruption is discovered by the monitoring process, then a measure of the likely corruption of the remaining memory area on the computer platform can be determined by probabilistic methods.

By providing a reserve memory area containing files which can be sacrificed, if the computer platform is compromised by a hostile attack, e.g. a virus, then the sacrificial files stored in the reserve memory area are at least as likely to be affected as other user data files stored in the remaining portion of the memory of the computer platform. Thus any corruption of the files in the reserve memory area, if detected early enough, may give an indication to the trusted component that file corruption is occurring on the computer platform, in which case the trusted component can take action to limit the spread of corruption at an early stage, and preferably before damage is done to important data files stored in the remaining memory area of the computer platform.

Referring to Figure 4 of the drawings, there is illustrated schematically an internal architecture of trusted component 202. The trusted component comprises a processor 400, a volatile memory area 401, a non-volatile memory area 402, a memory area storing native code 403, and a memory area storing one or a plurality of cryptographic functions 404, the non-volatile memory 401, native code memory 403 and cryptographic memory 404 collectively comprising the second memory means hereinbefore referred to. The cryptographic functions 404 may include or comprise a source of random numbers.

Trusted component 202 comprises a completely independent computing entity from the computer platform. In the illustrated example, the trusted component shares a motherboard with the computer platform so that the trusted component is physically linked to the computer platform. In a preferred embodiment, the trusted component is physically distinct from the computer platform, that is to say it does not exist solely as a sub-functionality of the data processor and memory means comprising the computer platform, but exists separately as a separate physical data processor 400 and separate physical memory area 401, 402, 403, 404. By providing a physically separate trusted component, the trusted component becomes more difficult to mimic or forge through software introduced onto the computer platform. Programs within the trusted component are pre-loaded at manufacture of the trusted component, and are not generally user configurable. The physicality of the trusted component, and the fact that the trusted component is not configurable by the user enables the user to have confidence in the inherent integrity of the trusted component, and therefore a high degree of "trust" in the operation and presence of the trusted component on the computer platform.

The user's smart card may comprise a "cash card" or a "crypto card", the functions of which are described in PCT/GB00/00751.

On each individual smart card may be stored a corresponding respective security data which is different for each smart card. For user interactions with the trusted component, e.g. for a dialogue box monitor display generated by the trusted component, the trusted component takes the security data (e.g. image data) from the user's smart card, and displays it in, or uses it as a background to the dialogue box displayed on the monitor 100. Thus, the user has confidence that the dialogue box displayed on the monitor 100 is generated by the trusted component.

Referring to Figure 5 of the drawings, an exemplary embodiment of an information system according to the present invention is based on the trusted computing platform principle described above. Thus, the information system comprises at least a monitor or screen 500, an input entry device, such as a keyboard, 501 and/or a pointing device, such as a mouse or trackball device, 505, a smart card reader 503, a confirmation key 504, and a main motherboard 600.

The main motherboard may be manufactured comprising a processor 601, a preferably permanently fixed trusted component 602, a memory device 700 local to the processor 601, a smart card interface 705, one or more control lines 702, one or more address lines 703, a confirmation key interface 706, and a databus 704 connecting the processor 601, trusted component 602, memory area 700, and smart card interface 705.

Referring to Figure 6 of the drawings, the information system 800 of Figure 5 is located in a prominent position in the predetermined area of interest, e.g. at the reception desk of a building, and is connected to, or includes integrally therein, a database 801 in which is stored information relating to computing platforms within the building and their security attributes. The information system may also be linked or connected to one or more of the computing platforms 802a-802n, and optionally to an external link 804 such as the Internet.

In use, a visitor to a building first identifies an information system according to the invention, which may be accompanied by some form of written statement by the service provider attesting the trustworthiness of the system. Thus, the statement may read "Organisation XYZ attests that this equipment is a Trusted System. This means that the organisation has taken every reasonable step to ensure the trustworthiness of information provided or published by the system, to ensure the trustworthiness of the verification services provided by the system and to ensure that the system maintains the privacy of its users".

Having located the information system, the visitor presents his/her personal computing platform or apparatus to the system and authorises the personal computing apparatus to interact with the information system. The personal computing apparatus could, for example, be a smart card or laptop computer. Communications between the system and the personal computing apparatus must be unambiguous, i.e. it must be obvious which information system is communicating with the computing apparatus.. Thus, the system must be a contact device or use, for example, directional wireless communication, such as IR. In any event, if the personal computing apparatus is a smart card, the interaction authorisation step may consist of entering into the information system a Personal Identification Number (PIN) which is then forwarded to the smart card for verification.

In some circumstances, such as within the premises of a private organisation, it may be desirable for the information system to verify the identity of the visitor before commencing communication. Such verification may take the form of a cryptographic challenge by the information system, i.e. a request for a password or code to be entered, in response to which the visitor (or his/her personal computing apparatus) must enter the correct password or code before communication will continue. This step may, however, be unnecessary or undesirable in public buildings such as libraries and museums, for example.

Once the authorisation and verification process has been completed, the information system provides information about computer platforms within the building, together with their security attributes where appropriate, and also indicates any additional services which the system provides. At least the information regarding the additional services available to the visitor is preferably presented on the monitor or screen of the system, although, the system itself may not have a screen, in which case such information may be displayed on the screen of the visitor's personal computing apparatus, where appropriate. In any event, the system provides the information regarding computer platforms within the predetermined area to the visitor's personal computing apparatus.

The additional services offered by the information system may permit the visitor to perform operations on the information provided by the system and/or to perform remote operations upon the information provided by the system, and report the results back to the visitor. For example, the information system may have greater computational power than the visitor's personal computing apparatus, in which case, the visitor may ask the information system to communicate with another service of the visitor's choosing (e.g. the visitor's smart card may ask the system to send the provided information to a service that is trusted by the visitor). The service would examine the information and return the results to the information system, which would forward the results to the visitor's personal computing apparatus. Of course, the information provided to the visitor may depend on the identity and/or level of authorisation of the visitor.

The visitor can then use the information provided by the information system during his/her visit to the building (or other predetermined area) of interest. When leaving the building, the visitor may once again present their personal computing apparatus to the information system so that the system can erase the building information from the visitor's personal computing apparatus. In any event, the system is preferably arranged to not to retain any unnecessary information relating to the visitor, thereby maintaining a high degree of privacy for the visitor.

In one particularly preferred exemplary embodiment of the invention, the information system is arranged to only provide details of trusted computing platforms within the predetermined area of interest. The visitor's personal computing apparatus (preferably a smart card or the like) may ask the information system to send that information to the visitor's verification service, which does the computationally intensive work of verifying identities and their associated certificates. The verification service would sign its conclusions and send the results back to the visitor's personal computing apparatus via the information system, so that the visitor's personal computing apparatus can then identify the platforms in the area which can be trusted by the visitor.

In general, the implementation of the information system of the invention must be trustworthy and, as such, should be designed and built such that its operations cannot be subverted. It may, for example, be incapable of executing any function other than one built into it. It may have physical protection to minimise the chance of physical alteration and/or it may periodically execute a self-test algorithm and report the result to a control centre. Alternatively or additionally, it may periodically execute a cryptographic challenge /response protocol to a control centre to request permission to operate, and stop operating if such permission is not forthcoming.

Embodiments of the present invention have been described above by way of examples only and it will be apparent to persons skilled in the art that modifications and variations can be made to the described embodiments without departing from the scope of the invention as defined by the appended claims.

CLAIMS

1) An information system comprising an information access point including means for retrieving information relating to computing platforms located within a pre-determined area, together with security attributes thereof, and means for providing said information to a user upon request.

2) A system according to Claim 1, wherein said means for providing information is arranged to provide only details and/or a list of public keys of genuine trusted computing platforms within said pre-determined area.

3) A system according to Claim 1 or Claim 2, wherein said information access point comprises a trusted computing platform.

4) A system according to any one of the preceding Claims comprising means for communicating or interacting with a user's portable computing apparatus.

5) A system according to Claim 4, wherein said means for communicating or interacting with a user's portable computing apparatus comprises physical contact means, such as a contact reader, or directional wireless communication.

6) A system according to any one of the preceding claims incorporating or accompanied by a declaration concerning the trustworthiness of the system.

7) A system according to claim 6, wherein said declaration is capable of interpretation by a user without preprocessing by an information processing

system.

8) A system according to any one of the preceding Claims, including means for verifying the identify of the user.

9) A system according to any one of the preceding Claims, including means to enable the user to perform operations, either locally or remotely, upon the information provided thereby.

10) An information system comprising a computing platform having a trusted component, means for communicating with a user's portable computing apparatus, means for retrieving information relating to a pre-determined area and communicating said information to said user's portable computing apparatus upon request.

11) An information system substantially as herein described with reference to the accompanying drawings.

ABSTRACT

A trusted service which publishes information describing security attributes of computing platforms in a defined physical area, for use by a visitor to a building, for example, who is unfamiliar with the computing platforms available for use therein. In a preferred embodiment, the system provides only details and/or a list of public keys of genuine trusted computing platforms within the area.

In another embodiment of the invention, the information system comprises a trusted computing platform for providing selected information to a user's portable computing apparatus.

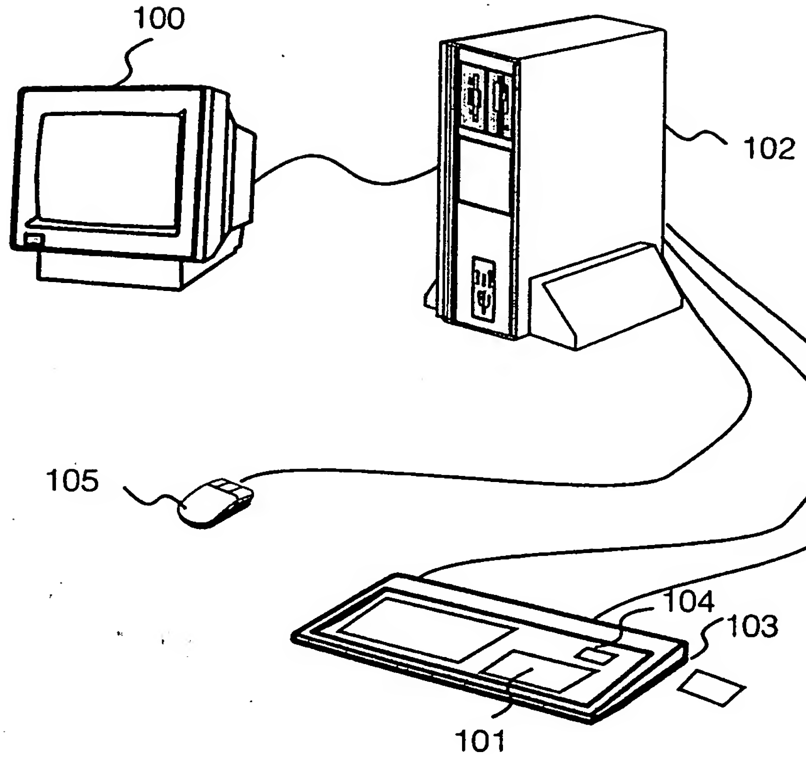

Fig. 1

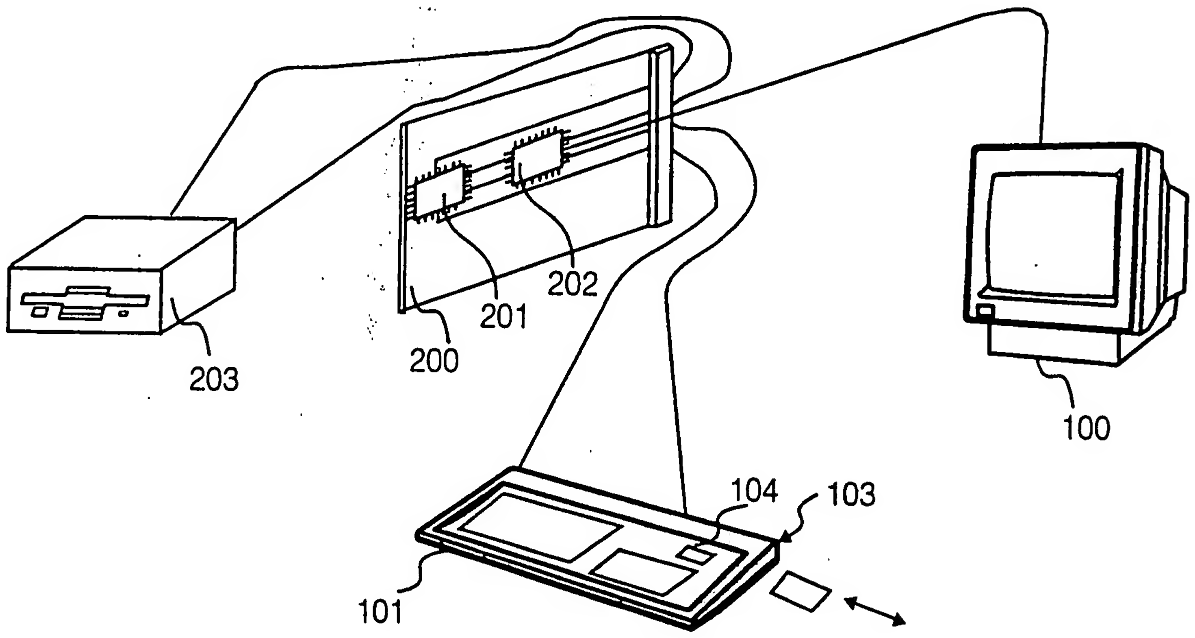

Fig. 2

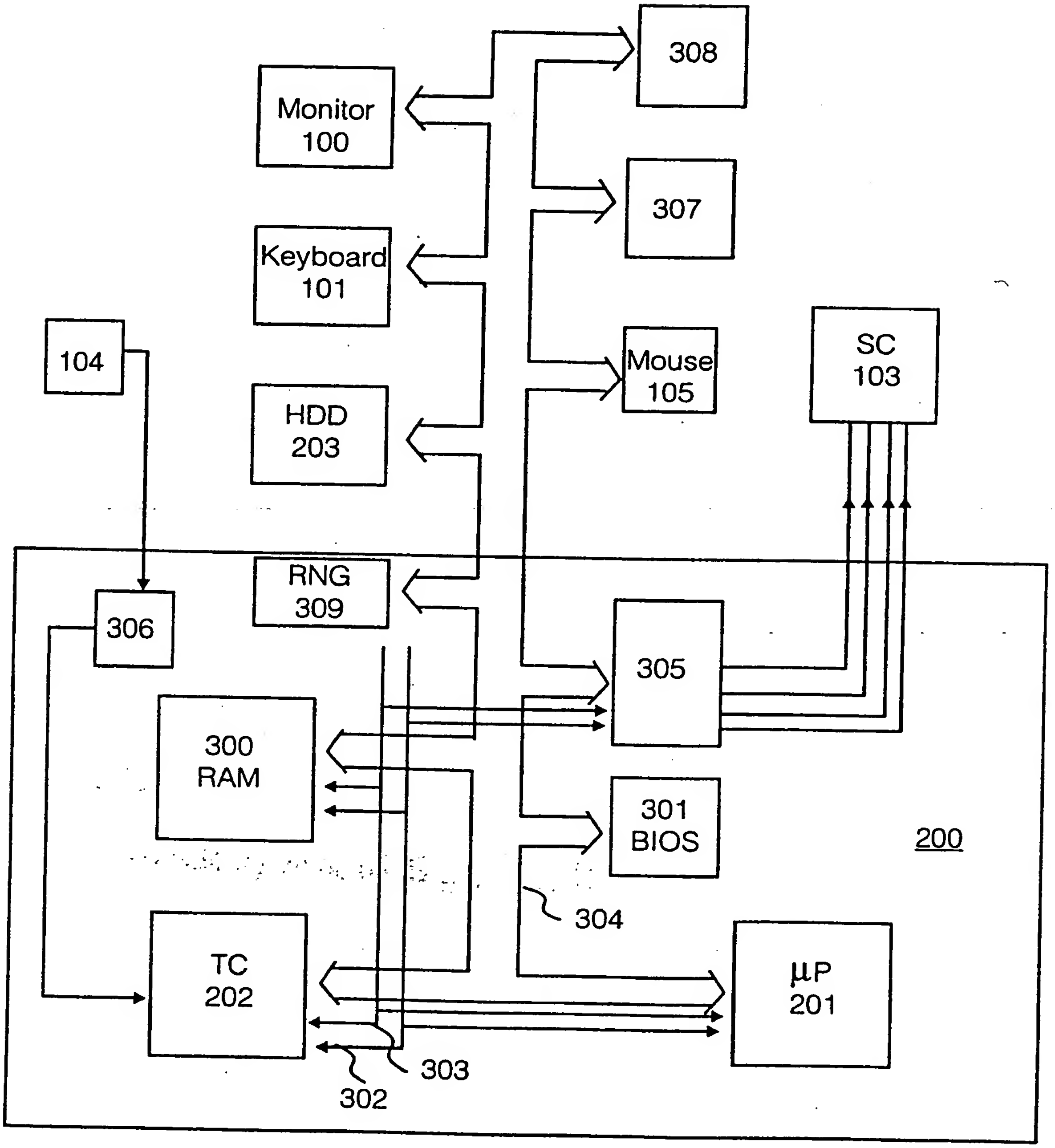
308
Monitor 100
307
Keyboard 101
104
Mouse 105
SC 103
HDD 203
RNG 309
306
305
300 RAM
301 BIOS
200
304
TC 202
µP 201
303
302

Fig. 3

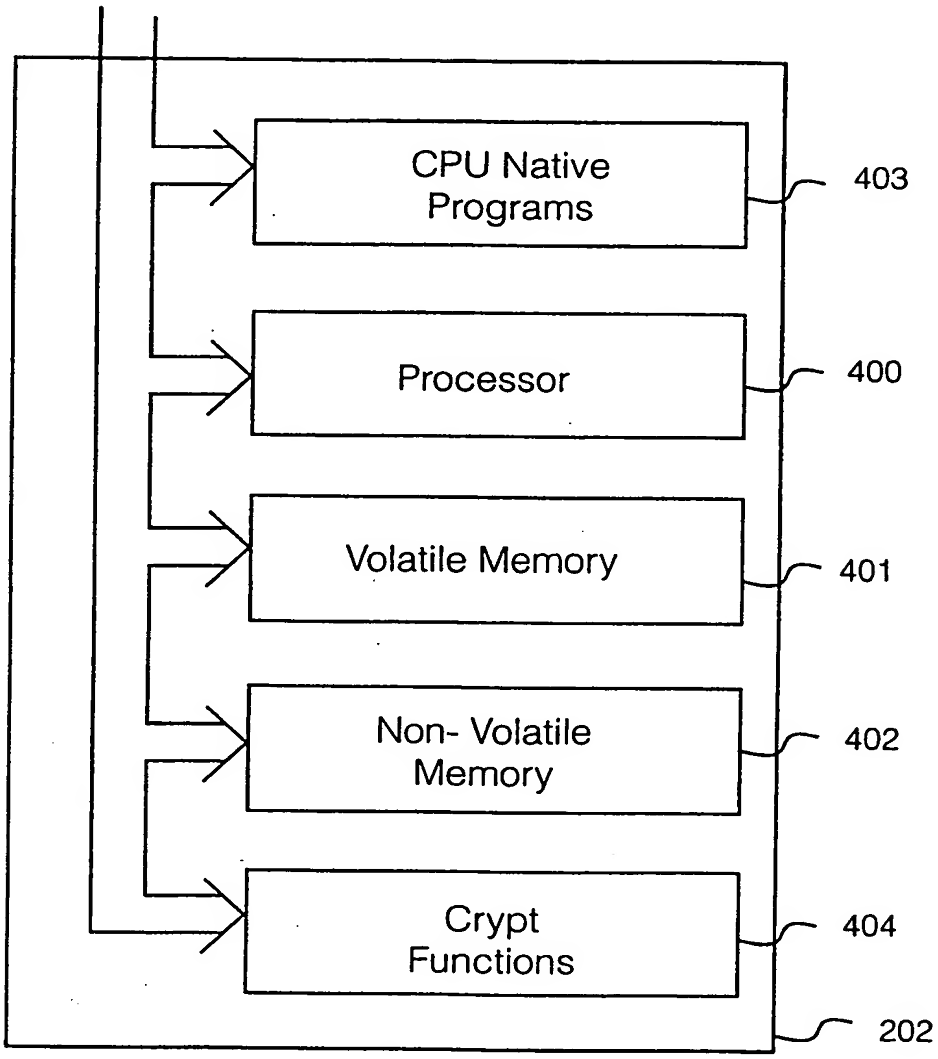
CPU Native Programs
403
Processor
400
Volatile Memory
401
Non- Volatile Memory
402
Crypt Functions
404
202

Fig. 4

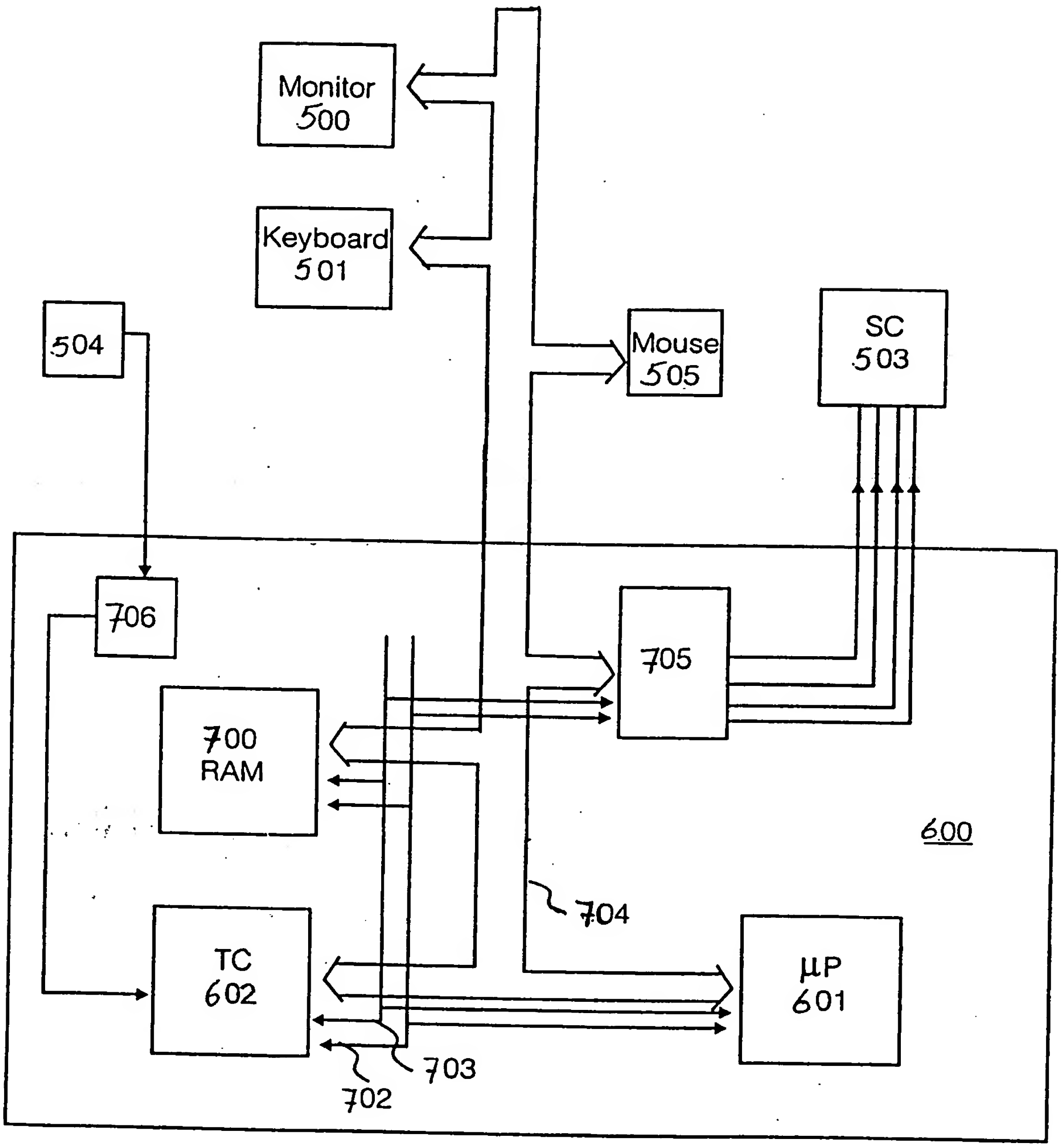
Monitor
500
Keyboard
501
504
Mouse
505
SC
503
706
705
700
RAM
600
704
TC
602
µP
601
703
702

Fig. 5

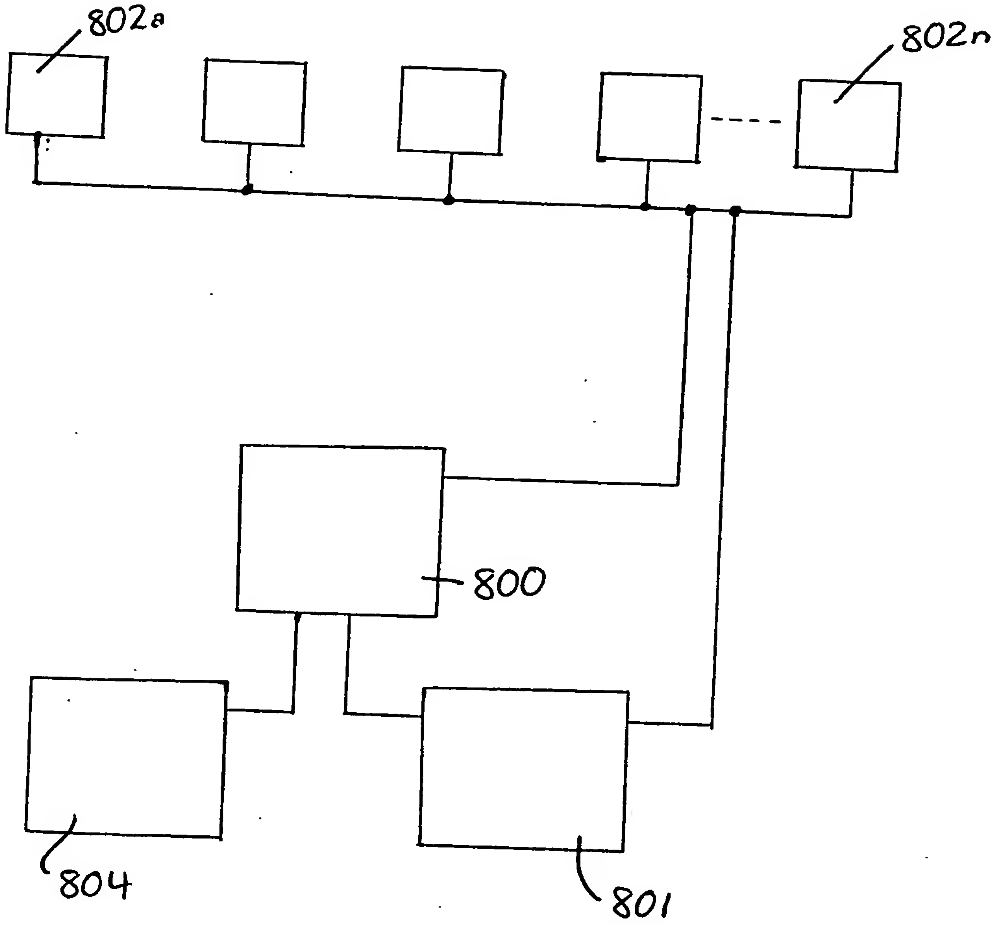

FIG. 6